View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

JOURNAL OF NUMBER THEORY 15, 164–181 (1982)

On the Irreducibility of a Class of Polynomials, III

K. GYŐRY

Mathematical Institute, Kossuth Lajos University, 4010 Debrecen, Hungary

Communicated by H. Zassenhaus

Received December 15, 1980; revised May 8, 1981

This work is a continuation and extension of our earlier articles on irreducible polynomials. We investigate the irreducibility of polynomials of the form $g(f(x))$ over an arbitrary but fixed totally real algebraic number field $\mathbb{L}$, where $g(x)$ and $f(x)$ are monic polynomials with integer coefficients in $\mathbb{L}$, g is irreducible over $\mathbb{L}$ and its splitting field is a totally imaginary quadratic extension of a totally real number field. A consequence of our main result is as follows. If g is fixed then, apart from certain exceptions f of bounded degree, $g(f(x))$ is irreducible over $\mathbb{L}$ for all f having distinct roots in a given totally real number field.

1. INTRODUCTION

Let $f(x)$ denote an arbitrary monic polynomial having distinct integer roots. I. Schur conjectured (see [22, 5]) that for $g(x) = x^{2^n} + 1$, $n \geqslant 1$, $g(f(x))$ is irreducible over the rational field $\mathbb{Q}$. Later Brauer *et al.* [6] posed the question of the irreducibility over $\mathbb{Q}$ of $g(f(x))$ for arbitrary irreducible polynomials $g(x) \in \mathbb{Z}[x]$ and showed that if $g(x)$ is of degree <4 and different from cx, then, up to the obvious translations $x \to x + a$ with $a \in \mathbb{Z}$, there are only finitely many $f(x)$ with distinct integer roots for which $g(f(x))$ is reducible and these f can be effectively determined. When $g(x)$ is linear, this statement can be deduced from an earlier theorem of Pólya [18].

Numerous authors obtained results in this direction (for references see, e.g., [6, 19, 25, 7, 8, 15]). For polynomials $g(x)$ of higher degree the first results were established by Seres [23–25]. In [25, 26] he proved Schur's conjecture in a more general form. Further, he solved [27] the Brauer–Hopf problem in the above sense for every $g(x)$ whose roots are complex units of a cyclotomic field.

In [7] the Brauer–Hopf problem has been settled for a much wider class of $g(x)$, namely for every monic polynomial $g(x)$ whose splitting field is a totally imaginary quadratic extension of a totally real number field.

0022-314X/82/050164–18$02.00/0

Copyright © 1982 by Academic Press, Inc.
All rights of reproduction in any form reserved.

Furthermore, the results of [25–27] have been generalized to these polynomials $g(x)$.

In [7, 8] we extended our investigations to the case when the $f \in \mathbb{Z}[x]$ are monic polynomials having distinct real roots. We showed [8] that in this more general situation one can get general irreducibility theorems only if $m = \deg(f)$ is large relative to the degree of the splitting field of f or if m is a prime, and we obtained [8] in both cases general results. In order to formulate and prove our irreducibility theorems we associated to every pair of polynomials f, g a certain graph with vertex set consisting of the roots of $f(x)$ and showed [7] that if this graph has a connected component with s vertices, then the number of irreducible factors of $g(f(x))$ is not greater than $[\deg(f)/s]$. Applying a theorem of Baker ([1]; see also [2]) concerning the Thue equation, we proved [8] that if $m = \deg(f)$ is sufficiently large relative to $g(0)$ and certain parameters of the splitting field of $f(x)$ then the graph in question has a connected component with at least $[(m+1)/2]$ vertices and so, in view of our estimate cited above, $g(f(x))$ is irreducible or the product of two irreducible factors of the same degree. We conjectured [8] that here the lower bound $[(m+1)/2]$ can be further improved (i.e., that for fixed $g(x)$, $g(f(x))$ is always irreducible if m is sufficiently large).

The resolution of a diophantine problem [12] enabled us to confirm [13] the above conjecture. In this paper, using our recent theorems [13] on the graphs mentioned above and a theorem of [11], we considerably improve and generalize the results of [25–27, 7, 8] concerning the Brauer–Hopf problem. We obtain general results on the irreducibility of polynomials of the form $g(f(x))$ over an arbitrary but fixed totally real algebraic number field $\mathbb{L}$, where $f(x)$ and $g(x)$ are monic polynomials with integer coefficients in $\mathbb{L}$, the roots of f are totally real and distinct, g is irreducible over $\mathbb{L}$ and its splitting field is a totally imaginary quadratic extension of a totally real number field. Our main result (Theorem 1) implies that if g is fixed then, apart from certain exceptions f of bounded degree, $g(f(x))$ is irreducible over $\mathbb{L}$ for all f having distinct roots in a fixed totally real number field. For polynomials g of the above type Theorem 1 may be regarded as a solution of a generalized version of the Brauer–Hopf problem.

We show that our theorems cannot be extended to arbitrary number fields $\mathbb{L}$ and to arbitrary irreducible polynomials $g(x)$ with integer coefficients in $\mathbb{L}$.

2. Notation

Before stating our theorems, we establish our notation and make some preliminary remarks.

Throughout Section 3 $\mathbb{L}$ and $\mathbb{K}$ denote totally real algebraic number fields with ring of integers $\mathbb{Z}_L$ and $\mathbb{Z}_K$, respectively. We suppose that $\mathbb{L} \subseteq \mathbb{K}$. Let l,

D_L and R_L (resp. k, D_K and R_K) be the degree, the discriminant and the regulator of $\mathbb{L}$ (resp. of $\mathbb{K}$). Let r denote the number of fundamental units in $\mathbb{K}$ and let $R_K^* = \max(R_K, e)$. We signify by $\psi_K(x)$ the number of pairwise non-associate algebraic integers β in $\mathbb{K}$ with $|N_{K/Q}(\beta)| \leqslant x$. We have (see [29])

$$\psi_K(x) \leqslant e^{20k^2} |D_K|^{1/(k+1)} (\log |2D_K|)^k x. \tag{1}$$

Let $f, g \in \mathbb{Z}_L[x]$. In order that $g(f(x))$ be irreducible over $\mathbb{L}$, it is necessary that $g(x)$ be irreducible over $\mathbb{L}$. However, this condition is not sufficient in general. Under the condition below concerning the splitting field of g we obtain general irreducibility theorems for the polynomials $g(f(x))$. In order to briefly state our theorems we introduce the following notation:

Let $G \geqslant 1$ denote an arbitrary constant and let $P_L(G)$ denote the set of monic polynomials $g \in \mathbb{Z}_L[x]$ having the following properties: g is irreducible over $\mathbb{L}$, the splitting field of g over $\mathbb{L}$ is a totally imaginary quadratic extension of a totally real number field and

$$|N_{L/Q}(g(0))|^{1/n} \leqslant G, \tag{2}$$

where $n = \deg(g)$.

It is obvious that, e.g., $P_Q(G)$ contains all cyclotomic polynomials and $P_L(G)$ contains infinitely many cyclotomic polynomials for every $G \geqslant 1$.

The polynomials f, $f^* \in \mathbb{Z}_L[x]$ will be called *$\mathbb{Z}_L$-equivalent* if $f(x) = f^*(x+a)$ with some $a \in \mathbb{Z}_L$. Clearly $g(f(x))$ and $g(f^*(x))$ are simultaneously reducible or irreducible over $\mathbb{L}$ for any $g \in \mathbb{Z}_L[x]$.

As usual, $\overline{|f|}$ will denote the maximum of the absolute values of the conjugates of the coefficients of a polynomial $f(x)$ with algebraic coefficients.

3. Theorems

First we show that if $g \in P_L(G)$ for some $G \geqslant 1$, then, apart from certain exceptions, $g(f(x))$ is irreducible over $\mathbb{L}$ for all $f \in \mathbb{Z}_L[x]$ having distinct roots in $\mathbb{K}$. To simplify the description of the exceptions we remark that among the polynomials f, g under consideration there exist monic polynomials $f, g \in \mathbb{Z}_L[x]$ with the following properties:

$$f(x) = f_1(x) f_2(x), \qquad \text{where} \quad f_1(x) - f_2(x) = t \in \mathbb{Z}_{L(t)},$$
$$f_i(x) - f_i(0) \in \mathbb{Z}_L[x], f_i(0) \in \mathbb{Z}_{L(t)},\ i = 1, 2, \tag{3}$$

and t is a non-zero totally real algebraic integer with $[\mathbb{L}(t):\mathbb{L}] \leqslant 2$. Each root $\beta \in \mathbb{C}$ of g satisfies

$$\beta = \varphi(\varphi - t), \tag{4}$$

where $\varphi + f_2(0) \in \mathbb{Z}_{L(\beta)}$ with some non-zero $\varphi \in \mathbb{Z}_{L(\beta,t)}$.

It is easy to see that, e.g., $f(x) = (x+t)x$ $(0 \neq t \in \mathbb{Z}_L)$ and the minimal polynomial $g(x)$ of $i(i-t)$ over $\mathbb{L}$ satisfy (3) and (4). Further, if $\sqrt{d} \in \mathbb{K}$ for some non-zero $d \in \mathbb{Z}_L$ and $a^2 - db^2 = t$ with non-zero $a, b \in \mathbb{Z}_L$, then $f(x) = (x^2 - 2ax + t)(x^2 - 2ax)$ and the above $g(x)$ also have the required properties. Further (more complicated) examples can be found in [8].

In the case of polynomials f, g having the properties (3) and (4)

$$f(x) - \beta = (f_1(x) - \varphi)(f_2(x) + \varphi)$$

over $\mathbb{L}(\beta)$ and so, by Lemma 1, $g(f(x))$ is reducible over $\mathbb{L}$. Further, if $g \in P_L(G)$, then by Lemma 2 $|N_{L(t)/Q}(t)| \leqslant (2^l G)^{[L(t):L]}$.

Our main result is then as follows:

THEOREM 1. *Let $\mathbb{L}$, $\mathbb{K}$ and $P_L(G)$ be as above, and let $f \in \mathbb{Z}_L[x]$ be a monic polynomial of degree m with distinct roots in $\mathbb{K}$. If $g(f(x))$ is reducible over $\mathbb{L}$ for some $g \in P_L(G)$ then*

(i) *m is even and $\leqslant 2(r+1)\,\psi_K^2(C)$, f is of the form* (3), *each root of g satisfies* (4) *and $g(f(x))$ is the product of two irreducible factors of equal degree, or*

(ii) *$2 \leqslant m \leqslant 2C^5$, f is $\mathbb{Z}_L$-equivalent to a polynomial of the form $\eta^m f^*(\eta^{-1}x) \in \mathbb{Z}_L[x]$, where η is a unit in $\mathbb{L}$, $f^* \in \mathbb{Z}_L[x]$ satisfies*

$$\overline{|f^*|} < \exp\{m(k+2)\,C^{10}(\log C)^4\} \tag{5}$$

with

$$C = \max\{(2G^{2/l})^k, |D_K|^{k^2}(\log|2D_K|)^{2r/5} \times \exp[(25(r+3)k)^{20(r+2)} R_K^2 \log R_K^*]\}$$

and $g^*(f^*(x))$ is reducible over $\mathbb{L}$ where

$$g^*(x) = \eta^{-mn} g(\eta^m x) \in P_L(G), \qquad n = \deg(g).$$

For $\mathbb{L} = \mathbb{Q}$ and $[\mathbb{K}:\mathbb{Q}] \leqslant 2$ this result was proved in [7, 8] as a generalization of some theorems of Seres [25, 27], The special case $\mathbb{L} = \mathbb{Q}$ of Theorem 1 is a considerable improvement of the main result (Theorem 1a) of [8]. As remarked in the Introduction, in case of polynomials $g \in P_L(G)$ our above theorem may be regarded as a solution of a generalization of the Brauer–Hopf problem.

As we mentioned, there exist polynomials f, g with property (i) and these exceptions are connected with the Tarry–Escott problem (cf. [21, 8]). Further, for suitably chosen $\mathbb{L}$ and $\mathbb{K}$ there are infinitely many g and, for each of these g, there are infinitely many pairwise inequivalent f such that f, g have the property (i), but do not have the property (ii). This is the case, e.g., if $\mathbb{L} = \mathbb{Q}$ and $\mathbb{K}$ contains a quadratic subfield (see [8] and the second example given before Theorem 1). In these examples $t \in \mathbb{Z}_L$, but it is easy to construct polynomials f, g satisfying (i) with $t \notin \mathbb{L}$. Finally we remark that for suitable f there are infinitely many g for which (i) holds.

There exists $f \in \mathbb{Z}_L[x]$ such that f, g have property (ii) for infinitely many $g \in P_L(G)$ (see, e.g., the exceptions in Theorem 6 of [7]). Apart from the exceptions f, g described in (i), Theorem 1 reduces the question of the irreducibility of polynomials $g(f(x))$ in question to that of the irreducibility of $g(f^*(x))$, where the polynomials $f^* \in \mathbb{Z}_L[x]$ satisfy (5) and $\deg(f^*) = m \leqslant 2C^5$. Clearly there are only finitely many f^* with these properties and these f^* can be effectively determined.

It is evident that in case (ii) the reducibility of $g^*(f^*(x))$ implies the reducibility of $g(f(x))$. By using a well-known algorithm of Zassenhaus [31] we can check whether $g^*(f^*(x))$ is reducible over $\mathbb{L}$.

Since $R_K \geqslant 0, 373$ (see [17]), from (1) we get $2(r+1)\ \psi_K^2(C) \leqslant C^3$ and Theorem 1 yields the following:

COROLLARY. *Let $f(x)$, C and $P_L(G)$ be as in Theorem 1. If $\deg(f) > 2C^5$ then $g(f(x))$ is irreducible over $\mathbb{L}$ for every $g \in P_L(G)$.*

This corollary also improves and generalizes the main result of [8].

It is easy to verify that if $p \in \mathbb{Z}_L[x]$ is a monic irreducible polynomial over $\mathbb{L}$, its splitting field is totally real, $a_1, ..., a_m \in \mathbb{Z}_L$ are distinct and m is sufficiently large then $f(x) = p(x + a_1) \cdots p(x + a_m)$ satisfies the conditions of the above corollary.

THEOREM 2. *Let $\mathbb{L}$, $\mathbb{K}$, C and $P_L(G)$ be defined as in Theorem 1, and let $f \in \mathbb{Z}_L[x]$ be a monic polynomial with more than $\max(\deg(f)/2 + 1,\ 2C^5)$ distinct roots in $\mathbb{K}$. Then $g(f(x))$ is irreducible over $\mathbb{L}$ for every $g \in P_L(G)$.*

In the case $\mathbb{L} = \mathbb{K} = \mathbb{Q}$ a slightly more precise result was established in [7].

Theorem 2 also constains the above corollary of Theorem 1.

Our Theorems 1 and 2 do not remain valid for any number field $\mathbb{L}$ and for any monic irreducible polynomial $g \in \mathbb{Z}_L[x]$. Indeed, let $\mathbb{L} \subseteq \mathbb{K}$ be any (not necessarily totally real) algebraic number fields having infinitely many units, $f \in \mathbb{Z}_L[x]$ a monic polynomial of degree m whose roots are distinct units of $\mathbb{K}$ and $g(x) = x - f(0)$. Then $|N_{L/Q}(g(0))| = 1$, m can be arbitrarily large relative to C and $x \mid g(f(x))$ in $\mathbb{Z}_L[x]$.

We consider next the case when the polynomials $f \in \mathbb{Z}_L[x]$ are of prime degree. As usual, $D(f)$ will denote the discriminant of a polynomial $f(x)$.

THEOREM 3. *Let $\mathbb{L}$ and $P_L(G)$ be as in Theorem* 1, *and let $f \in \mathbb{Z}_L[x]$ be a monic irreducible polynomial over $\mathbb{L}$ with totally real splitting field. If* $\deg(f) = p$ *is a prime and*

$$|N_{L/Q}(D(f))| > (2^l G)^{p(p-1)} \tag{6}$$

then $g(f(x))$ is irreducible over $\mathbb{L}$ for every $g \in P_L(G)$.

The case of Theorem 3 when $\mathbb{L} = \mathbb{Q}$ was proved in [8].

Theorem 3 together with Theorem 1 of [11] gives the following:

THEOREM 4. *Let $\mathbb{L}$ and $P_L(G)$ be as in Theorem* 1, *and let $f \in \mathbb{Z}_L[x]$ be a monic irreducible polynomial over $\mathbb{L}$ with totally real splitting field. If* $\deg(f) = p$ *is a prime and $g(f(x))$ is reducible over $\mathbb{L}$ for some $g \in P_L(G)$, then f is $\mathbb{Z}_L$-equivalent to a polynomial of the form $\eta^p f^*(\eta^{-1}x)$, where η is a unit, $f^* \in \mathbb{Z}_L[x]$ satisfies*

$$\overline{|f^*|} < \exp\{c_1[(|D_L| G^{p-1})^{3/2}(\log|2D_L G|)^{l+1}]^{4p^3}\} \tag{7}$$

with an effectively computable positive constant $c_1 = c_1(l, p)$ and $g^*(f^*(x))$ is reducible over $\mathbb{L}$, where $g^*(x) = \eta^{-pn} g(\eta^p x) \in P_L(G)$, $n = \deg(g)$.

Our Theorem 4 generalizes Theorem 2a of [8] and Theorem 4 of [10].

There are only finitely many $f^* \in \mathbb{Z}_L[x]$ of degree p with the property (7) and all these f^* can be effectively determined. Similarly to Theorem 1, Theorem 4 reduces the problem of the irreducibility of polynomials $g(f(x))$ of the type considered to the case of the polynomials $g(f^*(x))$.

Proposition 6 of [8] shows that our Theorems 3 and 4 cannot be extended to polynomials f of composite degree. Further, Theorems 3 and 4 do not remain true if the splitting field of f or of g does not possess the required property (see, e.g., Proposition 7 in [8]).

4. LEMMAS

To prove our theorems we need some lemmas. We keep the notations of Section 3, but without assuming that the fields $\mathbb{L}$, $\mathbb{K}$ are totally real.

LEMMA 1. (Capelli). *Let $\mathbb{L}$ be any algebraic number field, $f, g \in \mathbb{Z}_L[x]$ monic polynomials, g irreducible over $\mathbb{L}$ and β one of the roots of g in $\mathbb{C}$. If*

$$f(x) - \beta = \prod_{i=1}^{s} (\pi_i(x))^{k_i}$$

is the irreducible factorization of $f(x)-\beta$ *over* $\mathbb{L}(\beta)$ *then*

$$g(f(x)) = \prod_{i=1}^{s} (N(\pi_i(x)))^{k_i} \qquad (N \text{ denotes } N_{L(\beta)(x)/L(x)})$$

is the irreducible factorization of $g(f(x))$ *over* $\mathbb{L}$.

Proof. See [30] or [20]. We remark that Capelli proved this theorem in a less general form (cf. [30]).

LEMMA 2. *Let* $\mathbb{M}$ *be a totally imaginary quadratic extension of a totally real algebraic number field, and let* α *and* β *be non-zero algebraic integers in* $\mathbb{M}$. *If* α/β *is not real and* $\alpha+\beta$ *is real then*

$$N_{M/Q}\left(\frac{\alpha+\beta}{2}\right) \leqslant N_{M/Q}(\alpha\beta).$$

Proof. This is Corollary 3.2 in [9].

Let $\mathbb{M}$ be an arbitrary algebraic number field, and let $\mathscr{A} = \{\alpha_1,..., \alpha_m\}$ be a finite subset of $\mathbb{Z}_M$. Using the terminology of [4], for given $N \geqslant 1$ we denote by $\mathscr{G}_M(\mathscr{A}, N)$ the graph whose vertex set is $\mathscr{A}$ and whose edges are the unordered pairs $[\alpha_i, \alpha_j]$ having the property

$$|N_{M/Q}(\alpha_i - \alpha_j)| > N.$$

It is clear that the graph $\mathscr{G}_M(\mathscr{A}, N)$ defined above is uniquely determined by $\mathbb{M}$, $\mathscr{A}$ and N.

LEMMA 3. *Let* $\mathbb{M}$ *be as in Lemma* 2, $f_1 \in \mathbb{Z}_M[x]$ *a monic polynomial with real coefficients,* $\alpha_1,..., \alpha_s$ $s \geqslant 2$ *distinct real algebraic integers in* $\mathbb{M}$, *and* β *a non-real algebraic integer in* $\mathbb{M}$. *Let* $\mathscr{A} = \{\alpha_1,..., \alpha_s\}$, *and let* $\mathbb{M}' \supseteq \mathbb{M}$ *be any totally imaginary quadratic extension of a totally real algebraic number field. If the graph* $\mathscr{G}_M(\mathscr{A}, N_{M/Q}(2\beta))$ *is connected then* $F(x) = f_1(x)(x-\alpha_1)\cdots(x-\alpha_s)-\beta$ *has no irreducible factor of degree less than s over* $\mathbb{M}'$. *If in particular* $s > \deg(F)/2$, *then* $F(x)$ *is irreducible over* $\mathbb{M}'$.

Proof. This is Lemma 7 in [8]. It is not valid for arbitrary number fields $\mathbb{M}$, $\mathbb{M}'$ (see [7, 8]). Further, the estimate given for the degree of irreducible factors of F is in general best possible (cf. [8]).

Now let $\mathbb{K}$ be an arbitrary algebraic number field with the parameters specified in Section 2. Suppose

$$N \geqslant |D_K|^{k^2}(\log|2D_K|)^{2r/5} \exp\{(25(r+3)k)^{20(r+2)} R_K^2 \log R_K^*\} \tag{8}$$

and consider the graph $\mathscr{G}_K(\mathscr{A}, N)$, where $\mathscr{A} = \{\alpha_1, ..., \alpha_m\}$ is a finite subset of $\mathbb{Z}_K$ with $m \geqslant 2$ elements. Let $\overline{|\alpha|}$ denote the maximum of the absolute values of the conjugates of an algebraic number α.

Lemma 4. *Let N and $\mathscr{G}_K(\mathscr{A}, N)$ be as above. Then at least one of the following cases holds:*

(i) *$\mathscr{G}_K(\mathscr{A}, N)$ has a connected component with more than $m/2$ vertices,*

(ii) *m is even and $\leqslant 2(r+1)\psi_K^2(N)$, $\mathscr{G}_K(\mathscr{A}, N)$ has two connected components with $m/2$ vertices and both components are complete,*

(iii) *$m \leqslant 2N^5$ and there exist a unit ε in $\mathbb{K}$ and $\alpha_{ij} \in \mathbb{Z}_K$ such that $\alpha_i - \alpha_j = \varepsilon \alpha_{ij}$ for all $\alpha_i, \alpha_j \in \mathscr{A}$ and*

$$\max_{i,j} \overline{|\alpha_{ij}|} < \exp\{N^{10}(\log N)^4\}. \tag{9}$$

Proof. This lemma is a simple consequence of Theorems 1 and 2 of [13] (see also the remark after Theorem 1 in [13]).

Lemma 5. *Let $\mathscr{G}_K(\mathscr{A}, N)$ be defined as above with N satisfying* (8) *and suppose that the number m of vertices of $\mathscr{G}_K(\mathscr{A}, N)$ is greater than $2N^5$. Then $\mathscr{G}_K(\mathscr{A}, N)$ has a connected component with at least $m-1$ vertices.*

Proof. Lemma 5 is an immediate consequence of Theorem 2 of [13].

Lemma 6. *Let $\mathbb{M}$ and $\mathbb{M}'$ be as in Lemma* 3, *$\mathbb{K}$ a real subfield of $\mathbb{M}$, $\alpha_1, ..., \alpha_m$ $m \geqslant 2$ distinct algebraic integers in $\mathbb{K}$ and β a non-real algebraic integer in $\mathbb{M}$. Suppose that N satisfies* (8) *and $N \geqslant N_{M/Q}(2\beta^2)^{1/[M:K]}$. If $F(x) = (x-\alpha_1) \cdots (x-\alpha_m) - \beta$ is reducible over $\mathbb{M}'$ then*

(i) *m is even and $\leqslant 2(r+1)\psi_K^2(N)$, $(x-\alpha_1)\cdots(x-\alpha_m) = f_1(x) f_2(x)$ with $f_1(x) - f_2(x) = t \in \mathbb{Z}_K$ and $N_{M/Q}(t) \leqslant N_{M/Q}(2\beta)$, $\beta = \varphi(\varphi - t)$ with $\varphi \in \mathbb{Z}_{M'}$ and*

$$F(x) = (f_1(x) - \varphi)(f_2(x) + \varphi)$$

is the factorization of F into irreducible polynomials in $\mathbb{M}'[x]$, or

(ii) *$m \leqslant 2N^5$, there exist a unit $\varepsilon \in \mathbb{K}$ and $\alpha_{ij} \in \mathbb{Z}_K$ such that $\alpha_i - \alpha_j = \varepsilon\alpha_{ij}$ for all α_i, α_j and* (9) *holds.*

By the help of the example mentioned after Theorem 1 it is easy to show that in Lemma 6 both cases (i) and (ii) can occur.

In case (i) $\varphi + (t - \varphi) \in \mathbb{Z}_M$ and $-\beta = \varphi(t-\varphi) \in \mathbb{Z}_M$, hence either $\varphi \in \mathbb{Z}_M$ or φ is a quadratic algebraic integer over $\mathbb{M}$.

In case (ii) $F(x)$ is $\mathbb{Z}_K$-equivalent to $x(x-\varepsilon\alpha_{21})\cdots(x-\varepsilon\alpha_{m1})-\beta$ and this polynomial is reducible over $\mathbb{M}'$ if and only if $x(x-\alpha_{21})\cdots(x-\alpha_{m1})-\varepsilon^{-m}\beta$ is also reducible.

Proof of Lemma 6. We shall use some ideas of the proof of Theorem 1a of [8].

Suppose that $F(x)=(x-\alpha_1)\cdots(x-\alpha_m)-\beta$ is reducible over $\mathbb{M}'$. Write $\mathscr{A}=\{\alpha_1,\ldots,\alpha_m\}$ and consider the graphs $\mathscr{G}_K(\mathscr{A},N)$ and $\mathscr{G}_M(\mathscr{A},N_{M/Q}(2\beta))$. It follows from

$$|N_{K/Q}(\alpha_i-\alpha_j)|>N$$

that

$$N_{M/Q}(\alpha_i-\alpha_j)>N^{[M:K]}\geqslant N_{M/Q}(2\beta).$$

Hence any edge $[\alpha_i,\alpha_j]$ of $\mathscr{G}_K(\mathscr{A},N)$ is an edge of $\mathscr{G}_M(\mathscr{A},N_{M/Q}(2\beta))$. Since $F(x)$ is reducible, by Lemma 3 $\mathscr{G}_M(\mathscr{A},N_{M/Q}(2\beta))$ has no connected component with more than $m/2$ vertices and so $\mathscr{G}_K(\mathscr{A},N)$ has the same property. Consequently, by Lemma 4 $\mathscr{G}_K(\mathscr{A},N)$ has the properties (ii) or (iii) specified in Lemma 4.

First suppose that $\mathscr{G}_K(\mathscr{A},N)$ has the property (ii) occurring in Lemma 4, i.e., that m is even, say $m=2m'$, $m\leqslant 2(r+1)\,\psi_K^2(N)$, $\mathscr{G}_K(\mathscr{A},N)$ has two connected components with m' vertices and both components are complete. Since $\mathscr{G}_M(\mathscr{A},N_{M/Q}(2\beta))$ has no connected component with more than m' vertices, it has the same structure as $\mathscr{G}_K(\mathscr{A},N)$. Thus by Lemma 3 $F(x)$ is the product of two irreducible polynomials of degree m'over $\mathbb{M}'$. Suppose, for convenience, that $\alpha_1,\ldots,\alpha_{m'}$ and $\alpha_{m'+1},\ldots,\alpha_m$ are the vertex sets of the connected components of $\mathscr{G}_K(\mathscr{A},N)$. Write $f_1(x)=(x-\alpha_1)\cdots(x-\alpha_{m'})$, $f_2(x)=(x-\alpha_{m'+1})\cdots(x-\alpha_m)$ and

$$F(x)=f_1(x)\,f_2(x)-\beta=\pi_1(x)\,\pi_2(x), \tag{10}$$

where $\pi_1,\pi_2\in\mathbb{Z}_{M'}[x]$ are monic irreducible polynomials of degree m' over $\mathbb{M}'$. Then

$$\begin{aligned}\pi_1(x)&=f_1(x)+\varphi_{11}(x)=f_2(x)+\varphi_{12}(x),\\ \pi_2(x)&=f_1(x)+\varphi_{21}(x)=f_2(x)+\varphi_{22}(x),\end{aligned} \tag{11}$$

with polynomials $\varphi_{11}(x)$, $\varphi_{12}(x)$, $\varphi_{21}(x)$, $\varphi_{22}(x)\in\mathbb{Z}_{M'}[x]$ of degree $\leqslant m'-1$. By the definition of $f_1(x)$

$$\varphi_{11}(\alpha_i)=\pi_1(\alpha_i)\neq 0, \qquad i=1,\ldots,m'.$$

Since $[\alpha_i, \alpha_j]$ is an edge of $\mathscr{G}_K(\mathscr{A}, N)$ for all i, j with $1 \leqslant i, j \leqslant m'$, so

$$\begin{aligned} N_{M'/Q}(\alpha_i - \alpha_j) &> N^{[M':K]} \geqslant N_{M'/Q}(2\beta^2) \\ &= 2^{[M':Q]} N_{M'/Q}(\pi_1(\alpha_i)\, \pi_2(\alpha_i)\, \pi_1(\alpha_j)\, \pi_2(\alpha_j)) \\ &\geqslant 2^{[M':Q]} N_{M'/Q}(\pi_1(\alpha_i)\, \pi_1(\alpha_j)) \\ &= 2^{[M':Q]} N_{M'/Q}(\varphi_{11}(\alpha_i)\, \varphi_{11}(\alpha_j)) > 0. \end{aligned}$$

Consequently, by Lemma 5 of [8] we get

$$\overline{\varphi_{11}(x)} = \rho_{11} \varphi_{11}(x)$$

with some $\rho_{11} \in \mathbb{M}'$ (where $\overline{\varphi_{11}(x)}$ denotes the complex conjugate of $\varphi_{11}(x)$). We can prove in the same way as above that $\overline{\varphi_{12}(x)} = \rho_{12}\varphi_{12}(x)$, $\overline{\varphi_{21}(x)} = \rho_{21}\varphi_{21}(x)$ and $\overline{\varphi_{22}(x)} = \rho_{22}\varphi_{22}(x)$ with $\rho_{12}, \rho_{21}, \rho_{22} \in \mathbb{M}'$.

We follow now the argument of the proof of Theorem 1a of [8]. Equation (11) implies

$$\frac{\overline{\pi_1(\alpha_i)}}{\pi_1(\alpha_i)} = \frac{\overline{\varphi_{11}(\alpha_i)}}{\varphi_{11}(\alpha_i)} = \rho_{11} \quad \text{and} \quad \frac{\overline{\pi_2(\alpha_i)}}{\pi_2(\alpha_i)} = \frac{\overline{\varphi_{21}(\alpha_i)}}{\varphi_{21}(\alpha_i)} = \rho_{21}, \quad i = 1, ..., m'.$$

This together with (10) gives

$$\rho = \frac{\bar{\beta}}{\beta} = \frac{\overline{\pi_1(\alpha_i)\, \pi_2(\alpha_i)}}{\pi_1(\alpha_i)\, \pi_2(\alpha_i)} = \rho_{11}\rho_{21}$$

and similarly $\rho_{12}\rho_{22} = \rho$. In view of (11), (10) may be written in the form

$$\begin{aligned} & f_1(x) f_2(x) - \beta \\ &\quad = \pi_1(x)\, \pi_2(x) = \{f_1(x) + \varphi_{11}(x)\}\{f_2(x) + \varphi_{22}(x)\}, \end{aligned}$$

whence

$$-\beta = f_1(x)\, \varphi_{22}(x) + f_2(x)\, \varphi_{11}(x) + \varphi_{11}(x)\, \varphi_{22}(x). \tag{12}$$

By taking the complex conjugate of both sides we get

$$-\rho\beta = \rho_{22} f_1(x)\, \varphi_{22}(x) + \rho_{11} f_2(x)\, \varphi_{11}(x) + \rho_{11}\rho_{22}\varphi_{11}(x)\, \varphi_{22}(x). \tag{13}$$

It follows from (12) and (13) that

$$\varphi_{11}(x) \mid \rho\beta - \rho_{22}\beta = \rho_{22}\beta(\rho_{12} - 1).$$

If $\rho_{12} - 1 = 0$ then $\overline{\varphi_{12}(x)} = \varphi_{12}(x)$ and so, by (11), $\pi_1(x)$ is a polynomial with real coefficients. Thus (10) gives

$$\pi_1(x) \mid \beta - \bar{\beta} \neq 0,$$

which is a contradiction. Consequently $\rho_{22}\beta(\rho_{12} - 1) \neq 0$ and so $\varphi_{11}(x) = \varphi_{11} \in \mathbb{Z}_{M'}$. Similarly, $\varphi_{12}(x) = \varphi_{12}$, $\varphi_{21}(x) = \varphi_{21}$ and $\varphi_{22}(x) = \varphi_{22}$ are also non-zero algebraic integers in $\mathbb{M}'$.

From (11) we get

$$f_1(x) - f_2(x) = \varphi_{12} - \varphi_{11} = \varphi_{22} - \varphi_{21} = t, \tag{14}$$

where $0 \neq t \in \mathbb{Z}_K$. Now (12) and (14) imply

$$-\beta - \varphi_{22}(t + \varphi_{11}) = (\varphi_{11} + \varphi_{22}) f_2(x).$$

But the polynomial $f_2(x)$ is not constant, hence

$$-\beta - \varphi_{22}(t + \varphi_{11}) = 0, \qquad \varphi_{11} + \varphi_{22} = 0$$

and with the notation $-\varphi_{11} = \varphi_{22} = \varphi$ we get $\beta = \varphi(\varphi - t)$. Then

$$F(x) = (f_1(x) - \varphi)(f_2(x) + \varphi)$$

is the irreducible factorization of F over $\mathbb{M}'$, φ and $t - \varphi$ are non-zero algebraic integers in $\mathbb{M}'$ and $(t - \varphi)/\varphi$ is not real. Thus, by Lemma 2

$$N_{M'/Q}(t/2) \leqslant N_{M'/Q}(\varphi(t - \varphi)) = N_{M'/Q}(\beta),$$

whence

$$N_{M/Q}(t) \leqslant N_{M/Q}(2\beta).$$

Finally, if $\mathscr{G}_K(\mathscr{A}, N)$ has property (iii) specified in Lemma 4, then $F(x)$ satisfies the conditions listed in (ii) of Lemma 6 and this completes the proof of our lemma.

LEMMA 7. *Let* $\mathbb{M}$, $\mathbb{M}'$, $\mathbb{K}$ *and* β *be as in Lemma* 6. *Suppose that* N *satisfies* (8) *and* $N \geqslant N_{M/Q}(2\beta)^{1/[M:K]}$. *Let* $\alpha_1, \ldots, \alpha_s$ *be distinct algebraic integers in* $\mathbb{K}$, *and* $f_1 \in \mathbb{Z}_M[x]$ *a monic polynomial with real coefficients. If*

$$F(x) = f_1(x)(x - \alpha_1) \cdots (x - \alpha_s) - \beta$$

and

$$s > \max(\deg(F)/2 + 1, 2N^5)$$

then $F(x)$ *is irreducible over* $\mathbb{M}'$.

Proof. Write $\mathscr{A} = \{\alpha_1, \ldots, \alpha_s\}$ and consider the graphs $\mathscr{G}_K(\mathscr{A}, N)$ and $\mathscr{G}_M(\mathscr{A}, N_{M/Q}(2\beta))$. By the assumption we have $s > 2N^5$ and so, by Lemma 5, $\mathscr{G}_K(\mathscr{A}, N)$ has a connected component with at least $s-1$ vertices. But we can see in the same way as in the proof of Lema 6 that every edge of $\mathscr{G}_K(\mathscr{A}, N)$ is an edge of $\mathscr{G}_M(\mathscr{A}, N_{M/Q}(2\beta))$. Consequently, this latter graph also has a connected component with at least $s-1$ vertices. Since $s - 1 > \deg(F)/2$, by Lemma 3 $F(x)$ is irreducible over $\mathbb{M}'$.

LEMMA 8. *Let $\mathbb{L}$ be any algebraic number field with the parameters specified in Section* 2, *α a non-zero element in $\mathbb{L}$ with $|N_{L/Q}(\alpha)| = m$, and v a positive integer. There exists a unit η in $\mathbb{L}$ such that*

$$\overline{|\alpha\eta^v|} \leqslant m^{1/l} \exp\{v(6l^3)^{l-1}R_L\}.$$

Proof. This lemma is a consequence of Lemma 3 of [14].

LEMMA 9. *Let $\mathbb{L}$ be as in Lemma* 8, *and let $f \in \mathbb{Z}_L[x]$ be a monic polynomial of degree $m \geqslant 2$ such that $0 < |N_{L/Q}(D(f))| \leqslant d$. Then f is $\mathbb{Z}_L$-equivalent to a polynomial of the form $\eta^m f^*(\eta^{-1}x)$, where η is a unit in $\mathbb{L}$, $f^* \in \mathbb{Z}_L[x]$ and*

$$\overline{|f^*|} < \exp\{c_2[(|D_L|\, d^{1/m})^{3/2}(\log|D_L d|)^{l+1}]^{4m^3}\}$$

with an effectively computable positive constant $c_2 = c_2(l, m)$.

Proof. Our Lemma 9 is a special case of Theorem 1 of [11] (see also (2′) in [11]).

5. Proofs of the Theorems

The proof of Theorem 1 will be based on Lemmas 6 and 1.

Proof of Theorem 1. Suppose that $f \in \mathbb{Z}_L[x]$ and $g \in P_L(G)$ satisfy the conditions of Theorem 1 and $g(f(x))$ is reducible over $\mathbb{L}$. Then $m \geqslant 2$. Let $\alpha_1, \ldots, \alpha_m$ denote the roots of f and let β be one of the roots of g. By Lemma 1 $F(x) = (x-\alpha_1)\cdots(x-\alpha_m) - \beta$ is reducible over $\mathbb{L}(\beta)$ and hence reducible also over $\mathbb{K}(\beta)$. Since $\mathbb{K}$ is totally real and the splitting field of g is a totally imaginary quadratic extension of a totally real field, $\mathbb{K}(\beta) = \mathbb{M}$ is also a totally imaginary quadratic extension of a totally real number field.

By virtue of (2) we have

$$\begin{aligned} |N_{M/Q}(2\beta^2)|^{1/[M:K]} &= 2^k\, |N_{L(\beta)/Q}(\beta)|^{2[M:L(\beta)]/[M:K]} \\ &= 2^k\, |N_{L/Q}(g(0))|^{2[M:L(\beta)]/[M:K]} \\ &\leqslant (2G^{2/l})^k \leqslant C \end{aligned}$$

with the C defined in Theorem 1. Consequently we may apply Lemma 6 with $\mathbb{M}' = \mathbb{M}$ and $N = C$, and we obtain that for $F(x)$ at least one of cases (i), (ii) of Lemma 6 holds.

First suppose that $F(x)$ possesses the properties specified by (i) of Lemma 6, i.e., $m = 2m'$, $m \leqslant 2(r+1)\,\psi_K^2(C)$, $(x-\alpha_1)\cdots(x-\alpha_m) = f_1(x) f_2(x)$ with $f_1(x) - f_2(x) = t \in \mathbb{Z}_K$, $\beta = \varphi(\varphi - t)$ with $0 \neq \varphi \in \mathbb{Z}_M$ and

$$F(x) = (f_1(x) - \varphi)(f_2(x) + \varphi)$$

is the decomposition of F into irreducible polynomials in $\mathbb{M}[x]$. Since $\mathbb{L}(\beta) \subseteq \mathbb{M}$ and $F(x)$ is reducible over $\mathbb{L}(\beta)$, this is at the same time the decompositions of F into irreducible polynomials over $\mathbb{L}(\beta)$. So, by Lemma 1, $g(f(x))$ is the product of two irreducible polynomials of degree $m' \deg(g)$ over $\mathbb{L}$.

Since $f_1(x) - f_2(x) = t$, f_1 and f_2 may be written in the form

$$f_1(x) = x^{m'} + a_1 x^{m'-1} + \cdots + a_{m'-1} x + f_1(0),$$
$$f_2(x) = x^{m'} + a_1 x^{m'-1} + \cdots + a_{m'-1} x + f_2(0).$$

Here f_1, $f_2 \in \mathbb{Z}_K[x]$. Further, in view of $f_1(x) f_2(x) \in \mathbb{Z}_L[x]$ we have $2a_1 \in \mathbb{Z}_L$. Thus $a_1 \in \mathbb{Z}_L$. We can prove by induction on j that $a_j \in \mathbb{Z}_L$ for $j = 1,\ldots, m'-1$ and $f_1(0) + f_2(0), f_1(0) f_2(0) \in \mathbb{Z}_L$. Since $f_1(0) - f_2(0) = t$, it follows that t is a totally real algebraic integer with $[\mathbb{L}(t) : \mathbb{L}] \leqslant 2$ and $f_i(0) \in \mathbb{Z}_{L(t)}$, $i = 1, 2$. This proves that f is of the form (3).

As we showed above, $f_2(x) + \varphi \in \mathbb{Z}_{L(\beta)}[x]$. Hence $f_2(0) + \varphi \in \mathbb{Z}_{L(\beta)}$, and so $\varphi \in \mathbb{Z}_{L(\beta, t)}$, i.e., (4) also holds.

Suppose now that for $F(x)$ case (ii) of Lemma 6 holds. Then $m \leqslant 2C^5$ and there exist a unit $\varepsilon \in \mathbb{K}$ and $\alpha_{ij} \in \mathbb{Z}_K$ such that for all distinct α_i, α_j

$$\alpha_i - \alpha_j = \varepsilon \alpha_{ij} \tag{15}$$

and

$$\max_{i,j} \overline{|\alpha_{ij}|} < \exp\{C^{10}(\log C)^4\}. \tag{16}$$

Evidently

$$0 \neq D(f) = \prod_{1 \leqslant i < j \leqslant m} (\alpha_i - \alpha_j)^2 \in \mathbb{Z}_L.$$

Further, by (15) and (16) we get

$$|N_{L/Q}(D(f))| \leqslant \exp\{lm(m-1)\, C^{10}(\log C)^4\} = C_1. \tag{17}$$

We could now apply Theorem 1 of [11] (or our Lemma 9 which is a particular case of that theorem) to f. However, following the argument of the proof of Theorem 1 of [11] we shall get much better and explicit bound in (5).

By virtue of Lemma 8 (17) implies that there exist a unit $\eta \in \mathbb{L}$ and a $\delta \in \mathbb{Z}_L$ such that $D(f) = \eta^{m(m-1)}\delta$ and

$$\overline{|\delta|} \leqslant C_1^{1/l} \exp\{m(m-1)(6l^3)^{l-1}R_L\} = C_2.$$

It follows from (15) that

$$(\varepsilon/\eta)^{m(m-1)} = \delta \prod_{1 \leqslant i < j \leqslant m} \alpha_{ij}^{-2},$$

whence

$$\begin{aligned}\overline{|\varepsilon/\eta|} &\leqslant C_2^{1/m(m-1)} \exp\{(k-1)\, C^{10}(\log C)^4\} \\ &= \exp\{kC^{10}(\log C)^4 + (6l^3)^{l-1}R_L\} = C_3.\end{aligned}$$

So from (15) we get

$$\alpha_i - \alpha_j = \eta\chi_{ij}, \qquad 1 \leqslant i < j \leqslant m, \tag{18}$$

with an algebraic integer $\chi_{ij} \in \mathbb{Z}_K$ satisfying

$$\max_{i,j} \overline{|\chi_{ij}|} \leqslant C_3 C_1^{1/lm(m-1)} = C_4.$$

Writing $\chi_{ii} = 0$, $\alpha_1 + \cdots + \alpha_m = a_1$ and $\chi_{i1} + \cdots + \chi_{im} = \vartheta_i$, from (18) we obtain

$$m\alpha_i = a_1 + \eta\vartheta_i, \qquad i = 1,..., m, \tag{19}$$

where $a_1 \in \mathbb{Z}_L$ and

$$\overline{|\vartheta_i|} \leqslant mC_4, \qquad i = 1,..., m. \tag{20}$$

Equation (19) gives

$$\eta\vartheta_i \equiv -a_1 (\operatorname{mod} m).$$

Since η, $a_1 \in \mathbb{Z}_L$, there is an $a_2 \in \mathbb{Z}_L$ such that

$$\vartheta_i \equiv a_2 \ (\operatorname{mod} m)$$

for each i, $i=1,\dots,m$. Further, by a result of Mahler [16] and Bartz [3] there exists an integral basis $\omega_1,\dots,\omega_l$ in $\mathbb{L}$ with the property

$$\max_{1\leqslant h\leqslant l} \overline{|\omega_l|} \leqslant l^l\,|D_L|^{1/2}.$$

Let us represent a_2 in such a basis. We can easily see that there is an $a_3\in\mathbb{Z}_L$ congruent to a_2 (mod m) for which

$$\overline{|a_3|} \leqslant ml^{l+1}\,|D_L|^{1/2}. \tag{21}$$

Write $\vartheta_i = a_3 + m\gamma_i$, $i=1,\dots,m$. Then γ_i is an algebraic integer for each i and by (20), (21), $l\leqslant k$ and $|D_L|\leqslant|D_K|$ we have

$$\max_i \overline{|\gamma_i|} \leqslant C_4 + l^{l+1}\,|D_L|^{1/2} \leqslant 2C_4. \tag{22}$$

Finally, from (19) we get

$$\alpha_i = a + \eta\gamma_i, \qquad i=1,\dots,m,$$

with a suitable algebraic integer a of $\mathbb{L}$.

Take now the polynomial

$$f^*(x) = \prod_{i=1}^{m} (x-\gamma_i).$$

Then $\eta^m f^*(\eta^{-1}x)\in\mathbb{Z}_L[x]$ is $\mathbb{Z}_L$-equivalent to f, $f^*\in\mathbb{Z}_L[x]$ and by (22)

$$\overline{|f^*|} < \exp\{m[(k+1)\,C^{10}(\log C)^4 + (6l^3)^{l-1}R_L]\}. \tag{23}$$

Using an explicit estimate of Siegel [28] we get

$$(6l^3)^{l-1}R_L < (6el^3)^l\,|D_L|^{1/2}(\log|2D_L|)^{l-1} \leqslant C$$

and (23) implies (5).

It is easily seen that $g^*(x) = \eta^{-mn}g(\eta^m x)\in P_L(G)$ and that $g^*(f^*(x))$ is reducible over $\mathbb{L}$.

Proof of Theorem 2. Let g be an arbitrary polynomial in $P_L(G)$, and let β be one of the roots of g in $\mathbb{C}$. Let $\mathbb{M}=\mathbb{K}(\beta)$. Then $\mathbb{M}$ is a totally imaginary quadratic extension of a totally real number field. In view of (2) we have

$$\begin{aligned} N_{M/Q}(2\beta)^{1/[M:K]} &= 2^k\,|N_{L(\beta)/Q}(\beta)|^{[M:L(\beta)]/[M:K]} \\ &= 2^k\,|N_{L/Q}(g(0))|^{[M:L(\beta)]/[M:K]} \\ &\leqslant (2G^{1/l})^k \leqslant C. \end{aligned}$$

Let $\alpha_1, \dots, \alpha_s$ denote the roots of f in $\mathbb{K}$, and write $f(x) = f_1(x)(x-\alpha_1) \cdots (x-\alpha_s)$. Since $f_1(x) \in \mathbb{Z}_K[x]$ is a monic polynomial and $s > \max(\deg(f)/2 + 1, 2C^5)$, by applying Lemma 7 to $f(x) - \beta$ with the choice $N = C$ we obtain that $f(x) - \beta$ is irreducible over $\mathbb{M}$. So it is irreducible over $\mathbb{L}(\beta)$, and by Lemma 1 $g(f(x))$ is irreducible over $\mathbb{L}$.

Proof of Theorem 3. Let g be an arbitrary polynomial in $P_L(G)$, β one of the roots of g and $\alpha_1, \dots, \alpha_p$ the roots of f in $\mathbb{C}$. Let $\mathbb{M} = \mathbb{L}(\alpha_1, \dots, \alpha_p, \beta)$. Then $\mathbb{M}$ is a totally imaginary quadratic extension of a totally real number field. Write $\mathscr{A} = \{\alpha_1, \dots, \alpha_p\}$ and consider the graph $\mathscr{G} = \mathscr{G}_M(\mathscr{A}, N_{M/Q}(2\beta))$.

Suppose, for convenience, that $\alpha_1, \dots, \alpha_s$ are the vertices of a maximal connected component of $\mathscr{G}$. In view of (6) and (2) we have

$$\begin{aligned}\prod_{1 \leqslant i < j \leqslant p} N^2_{M/Q}(\alpha_i - \alpha_j) &= |N_{L/Q}(D(f))|^{[M:L]} \\ &> (2^l G)^{p(p-1)[M:L]} \\ &\geqslant |N_{M/Q}(2\beta)|^{p(p-1)}.\end{aligned}$$

This implies

$$N_{M/Q}(\alpha_i - \alpha_j) > N_{M/Q}(2\beta)$$

for some i and j, and so $s \geqslant 2$.

Denoting by Γ the Galois group of $f(x)$ over $\mathbb{L}$, Γ may be regarded as a subgroup of the automorphism group of $\mathscr{G}$. So $\{\chi(\alpha_1), \dots, \chi(\alpha_s)\}$ and $\{\psi(\alpha_1), \dots, \psi(\alpha_s)\}$ are identical or disjoint for each $\chi, \psi \in \Gamma$ (where $\chi(\alpha_i)$ and $\psi(\alpha_i)$ denote the images of α_i under the automorphisms χ and ψ). Consequently there are $\chi_1, \dots, \chi_d \in \Gamma$ such that $\{\chi_1(\alpha_1), \dots, \chi_1(\alpha_s)\}, \dots, \{\chi_d(\alpha_1), \dots, \chi_d(\alpha_s)\}$ are pairwise disjoint and $p = ds$. Since $s \geqslant 2$ hence $s = p$ and so $\mathscr{G}$ is connected. Thus by Lemma 3 $f(x) - \beta$ is irreducible over $\mathbb{L}(\beta)$. Finally, Lemma 1 implies that $g(f(x))$ is irreducible over $\mathbb{L}$.

Proof of Theorem 4. Suppose that $f(x)$ satisfies the conditions of Theorem 4 and $g(f(x))$ is reducible over $\mathbb{L}$ for some $g \in P_L(G)$. Then by Theorem 3 we have

$$|N_{L/Q}(D(f))| \leqslant (2^l G)^{p(p-1)}.$$

So, by virtue of Lemma 9 f is $\mathbb{Z}_L$-equivalent to a polynomial of the form $\eta^p f^*(\eta^{-1}x)$, where $\eta \in \mathbb{L}$ is a unit, $f^* \in \mathbb{Z}_L[x]$ and (7) holds. Further $g^*(x) = \eta^{-pn} g(\eta^p x) \in P_L(G)$ and $g^*(f^*(x))$ is reducible over $\mathbb{L}$.

REFERENCES

1. A. BAKER, Bounds for the solutions of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.* **65**(1969), 439–444.
2. A. BAKER AND J. COATES, Integer points on curves of genus 1, *Proc. Cambridge Philos. Soc.* **67** (1970), 595–602.
3. K. M. BARTZ, On a theorem of Sokolovskiĭ, *Acta Arith.* **34** (1978), 113–126.
4. C. BERGE, "Graphs and Hypergraphs," North-Holland, Amsterdam/London, 1973.
5. A. BRAUER AND R. BRAUER, Über Irreduzibilitätskriterien von I. Schur and G. Pólya, *Math. Z.* **40** (1936), 242–265.
6. A. BRAUER, R. BRAUER, AND H. HOPF, Über die Irreduzibilität einiger spezieller Klassen von Polynomen, *Jahresber. Deutsch Math.-Verein.* **35** (1926), 99–112.
7. K. GYÖRY, Sur l'irréductibilité d'une classe des polynômes I, *Publ. Math. Debrecen* **18** (1971), 289–307.
8. K. GYÖRY, Sur l'irréductibilité d'une classe des polynômes II, *Publ. Math. Debrecen* **19** (1972), 293–326.
9. K. GYÖRY, Sur une classe des corps de nombres algébriques et ses applications, *Publ. Math. Debrecen* **22** (1975), 151–175.
10. K. GYÖRY, Sur les polynômes à coefficients entiers et de discriminant donné III, *Publ. Math. Debrecen* **23** (1976), 141–165.
11. K. GYÖRY, On polynomials with integers coefficients and given discriminant V. p-adic generalizations, *Acta Math. Acad. Sci. Hungar.* **32** (1978), 175–190.
12. K. GYÖRY, On the number of solutions of linear equations in units of an algebraic number field, *Comment. Math. Helv.* **54** (1979), 583–600.
13. K. GYÖRY, On certain graphs composed of algebraic integers of a number field and their applications I. *Publ. Math. Debrecen* **27** (1980), 229–242.
14. K. GYÖRY, On the solutions of linear diopantine equations in algebraic integers of bounded norm, *Ann. Univ. Budapest Eötvös, Sect. Math.* **22–23** (1979–1980), 225–233.
15. K. GYÖRY AND J. RIMÁN, On irreducibility criteria of Schur type (in Hungarian), *Mat. Lapok* **24** (1973), 225–253.
16. K. MAHLER, Inequalities for ideal bases in algebraic number fields, *J. Austral Math. Soc.* **4** (1964), 425–428.
17. M. POHST, Regulatorabschätzungen für total reelle algebraische Zahlkörper, *J. Number Theory* **9** (1977), 459–492.
18. G. PÓLYA, Verschiedene Bemerkungen zur Zahlentheorie, *Jahresber. Deutsch. Math-Verein.* **28** (1919), 31–40.
19. G. PÓLYA AND G. SZEGÖ, "Aufgaben und Lehrsätze aus der Analysis," Band II, Springer-Verlag, Berlin, 1925.
20. L. RÉDEI, "Algebra," Akadémiai Kiadó, Budapest, 1967.
21. W. SCHULZ, Über Reduzibilität bei gewissen Polynomen und das Tarry-Escottsche Problem, *Math. Z.* **63** (1955), 133–144.
22. I. SCHUR, Aufgabe 275, *Archiv Math. Phys.* **15** (1909), 259.
23. I. SERES, On the irreducibility of certain polynomials (in Hungarian), *Mat. Lapok* **3** (1952), 148–150.
24. I. SERES, Über eine Aufgabe von Schur, *Publ. Math. Debrecen* **3** (1953), 138–139.
25. I. SERES, Lösung und Verallgemeinerung eines Schurschen Irreduzibilitätsproblems für Polynome, *Acta Math. Acad. Sci. Hungar.* **7** (1956), 151–157.
26. I. SERES, Über die Irreduzibilität gewisser Polynome, *Acta Arith.* **8** (1963), 321–341.
27. I. SERES, Irreducibility of polynomials, *J. Algebra* **2** (1965), 283–286.
28. C. L. SIEGEL, Abschätzung von Einheiten, *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* (1969), 71–86.

29. J. S. Sunley, Class numbers of totally imaginary quadratic extensions of totally real fields, *Trans. Amer. Math. Soc.* **175** (1973), 209–232.
30. N. Tschebotaröw and H. Schwerdtfeger, "Grundzüge der Galois'schen Theorie," Noordhoff, Groningen/Djakarta, 1950.
31. H. Zassenhaus, On Hensel factorization, I, *J. Number Theory* **1** (1969), 291–311.